Assignment 4 – Wireshark Packet Analysis (Final Enhanced Version)

1. Setup & Installation

This section describes setting up Mininet and Wireshark for network packet analysis.

Wireshark Installation:

sudo apt update sudo apt install wireshark

Start Mininet:

sudo mn --topo single,2 --mac

2. Packet Capture Procedure

Using Wireshark on host h1, we capture ICMP packets generated by pinging h2.

Open host terminal:

xterm h1

Start Wireshark:

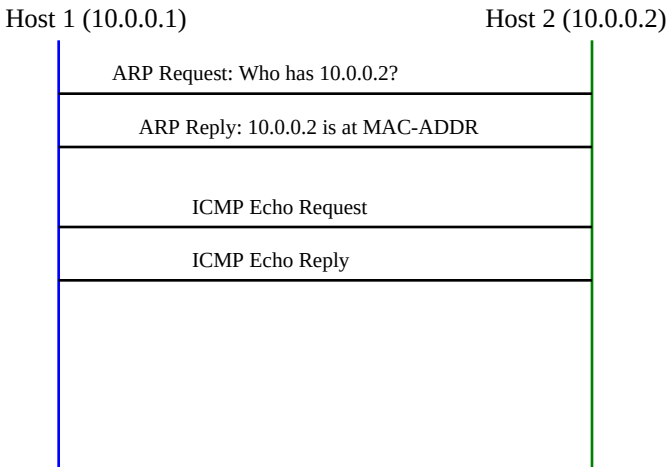
wireshark &

Ping from h1:

ping 10.0.0.2 -c 4

3. Time Diagram of Ping Operation

Below is an illustrated time diagram showing ARP and ICMP events:



4. Packet Header Analysis

Layer 2: Ethernet II

- Source MAC Address
- Destination MAC Address
- EtherType (0x0800 = IPv4)

Layer 3: IPv4 Header

- Version = 4
- Header Length
- TTL (Time To Live)
- Protocol = 1 (ICMP)
- Source IP Address
- Destination IP Address

Layer 4: ICMP Message

- Type (8=Request, 0=Reply)
- Code
- Identifier
- Sequence Number
- ICMP Payload

5. Learning Outcomes

- Understanding how ARP enables communication before IP transmission.
- Analyzing ICMP packets using Wireshark.
- Interpreting Layer 2, 3, and 4 headers.
- Drawing time-sequence diagrams for packet flow.